559,767

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 December 2004 (23.12.2004)

PCT

(10) International Publication Number
WO 2004/112306 A2

(51) International Patent Classification[7]: H04L 9/00

(21) International Application Number: PCT/IB2004/050813

(22) International Filing Date: 1 June 2004 (01.06.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
03101718.9 12 June 2003 (12.06.2003) EP

(71) Applicant *(for DE only)*: **PHILIPS INTELLECTUAL PROPERTY & STANDARDS GMBH** [DE/DE]; Steindamm 94, 20099 Hamburg (DE).

(71) Applicant *(for all designated States except DE, US)*: **KONINKLIJKE PHILIPS ELECTRONICS N. V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **AVANZI, Roberto** [IT/DE]; c/o Philips Intellectual Property &, Standards GmbH Weisshausstr. 2, 52066 Aachen (DE).

(74) Agent: **MEYER, Michael**; Philips Intellectual Property &, Standards GmbH Weisshausstr. 2, 52066 Aachen (DE).

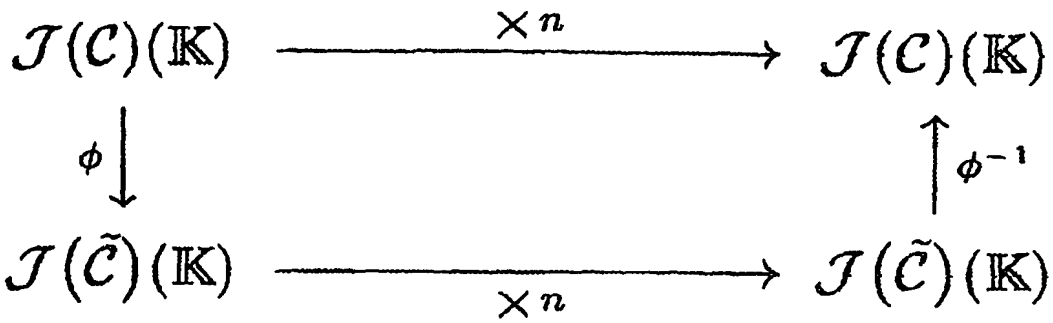
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD FOR DEFENCE AGAINST ATTACKS TAKING PLACE BY MEANS OF DIFFERENTIAL POWER ANALYSIS



(57) Abstract: In order to refine a method for defence against at least one attack made by means of differential power analysis on at least one hyperelliptic cryptosystem, in particular at least one hyperelliptic public key cryptosystem, which is given by at least one hyperelliptic curve (C) of any genus (g) over a finite field (K) in a first group, where the hyperelliptic curve (C) is given by at least one co-efficient, so that an essential contribution can be made towards an efficient and secure implementation of the hyperelliptic cryptosystem, it is proposed that the hyperelliptic curve (C) and/or at least one element of the first group, in particular at least one in particular reduced divisor and/or at least one intermediate result of a scalar multiplication, is randomised.

WO 2004/112306 A2